Please amend the claims as follows:

1-31. (Cancelled)

32. (Cancelled) A method of encrypting data, comprising:

choosing a modulus C for modular calculations, wherein C is a w-bit number, and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

using the modulus to encrypt data.

33. (Cancelled) The method of claim 32, further comprising:

performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) converting to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

34. (Cancelled) The method of claim 32, wherein the modulus C is of the form $2^w - L$, and wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

35. (Cancelled) The method of claim 34, further comprising:

calculating the modulus C by a process including

(a) splitting a number $P < 2^{2w}$ into 2 w-bit words H_1 and L_1;

(b) calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + ... + (H_1 2^{xk}) + H_1$, wherein $(w-3)/2 > x_1 > x_2 > ... > x_k > 0$ and $k << w$;

(c) splitting S_1 into two w-bit words H_2 and L_2;

(d) computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + ... + (H_2 2^{xk}) + H_2$;

(e) computing $S_3 = S_2 + (2^{x1} + ... + 2^{xk} + 1)$;

(f) determining the modulus C by comparing S_3 to 2w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$;

wherein the modulus C is a residue.

36. (Cancelled) The method of claim 32, wherein the modulus C is of the form $2^w + L$, and wherein the modulus C has a Hamming weight close to 1.

37. (Cancelled) The method of Claim 32, wherein the method of encrypting data comprises a method of cryptographic hashing.

38. (Cancelled) The method of Claim 32, wherein the modulus C is w-big and w-heavy.

39. (Cancelled) The method of Claim 32, wherein the modulus C is w-little and w-light.

40.(Cancelled) A method of encrypting data, comprising:

receiving data; and

using a modulus C to encrypt the data, wherein C is a w-bit number, wherein the modulus C is of the form $2^w - x$, wherein $x = \pm L$, wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$, and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

outputting the encrypted data.

41.(Cancelled) The method of claim 40, wherein the modulus C is w-big.

42.(Cancelled) The method of claim 40, wherein the modulus C is w-heavy.

43.(Cancelled) The method of claim 40, wherein the modulus C is w-little.

44.(Cancelled) The method of claim 40, wherein the modulus C is w-light.

45.(Cancelled) The method of claim 40, wherein $x = L$.

46.(Cancelled) The method of claim 40, wherein $x = - L$.

47. (Cancelled) The method of claim 40, wherein the step of encrypting the data includes the step of performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) converting to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

48. (Cancelled) The method of claim 40, further comprising:

calculating the modulus C by a process including

(a) providing a number $P < 2^{2w}$;

(b) splitting P into 2 w-bit words H_1 and L_1;

(c) calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$, wherein $(w-3)/2 > x_1 > x_2 > \ldots > x_k > 0$ and $k << w$;

(d) splitting S_1 into two w-bit words H_2 and L_2;

(e) computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

(f) computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

(g) determining the modulus C by comparing S_3 to 2w, wherein the modulus C is a residue, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$.

49. (Cancelled) The method of claim 40, wherein the modulus C has a Hamming weight close to 1.

50. (Cancelled) The method of Claim 40, wherein the method of encrypting data comprises a method of cryptographic hashing.

51. (Cancelled) The method of claim 32, wherein $C = 2^w - 2^{x1} - 2^{x2} - \ldots - 2^{xk} - 1$, wherein $(w - 3)/2 > x_1 > x_2 > \ldots > x_k > 0$, and wherein $k >> w$.

52. (Cancelled) The method of claim 32, further comprising:

choosing a first basis (m_1, m_2, ... m_t) and a second basis (m_{t+1}, m_{t+2}, ... m_{2t}), wherein m_1, ..., m_{2t} are moduli;

calculating a product $M = m_1 m_2 \ldots m_t$;

calculating a product $W = m_{t+1} m_{t+2} \ldots m_{2t}$; and

calculating a product ABM^{-1} mod p for n-bit numbers A and B by (a) computing Q mod M in the first basis such that AB + Qp = RM for some integral value R and for a number p which is prime relative to M and W; (b) converting Q to the second basis, Q mod W; and (c) computing R in the second basis, R mod W, wherein $R = (AB + Qp) M^{-1}$ mod W and R mod p = ABM^{-1} mod p.

53. (Cancelled) The method of claim 52 wherein, for i = 1 to 2t, $2^{k-1} \leq m_i \leq 2^k$, and wherein m_1, ..., m_{2t} are pairwise mutually prime.

54. (Cancelled) The method of claim 53, wherein $t \geq (n+1)/k$, where n is the bit length of the numbers being multiplied.

55. (Cancelled) The method of claim 54, wherein p is an n-bit number, and wherein p is a prime number.

56. (Cancelled) The method of claim 52, further comprising converting R to the first basis, R mod M.

57. (Cancelled) The method of claim 52, wherein the step of calculating a product ABM^{-1} mod p is performed iteratively and includes at least first and second subsequent iterations, and wherein the value of R calculated in the first iteration is utilized as the input value of R in the second iteration.

58. (Cancelled) The method of claim 52, wherein the data is encrypted using asymmetric encryption.

59. (Cancelled) The method of claim 52, wherein the data is encrypted using symmetric encryption.

60. (New) A method of encrypting data, comprising:

choosing a modulus C for modular calculations, wherein C is a w-bit number, and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

using the modulus to encrypt data;

wherein $C = 2^w - 2^{x1} - 2^{x2} - \ldots - 2^{xk} - 1$, wherein $(w - 3)/2 > x_1 > x_2 > \ldots > x_k > 0$, and wherein $k >> w$.

61. (New) The method of claim 60, further comprising:

performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) converting to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

62. (New) The method of claim 60, wherein the modulus C is of the form $2^w - L$, and wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

63. (New) The method of claim 62, further comprising:

calculating the modulus C by a process including

(a) splitting a number $P < 2^{2w}$ into 2 w-bit words H_1 and L_1;

(b) calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$, wherein $(w-3)/2 > x_1 > x_2 > \ldots > x_k > 0$ and $k << w$;

(c) splitting S_1 into two w-bit words H_2 and L_2;

(d) computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

(e) computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

(f) determining the modulus C by comparing S_3 to 2w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$;

wherein the modulus C is a residue.

64. (New) The method of claim 60, wherein the modulus C is of the form $2^w + L$, and wherein the modulus C has a Hamming weight close to 1.

65. (New) The method of Claim 60, wherein the method of encrypting data comprises a method of cryptographic hashing.

66. (New) The method of Claim 60, wherein the modulus C is w-big and w-heavy.

67. (New) The method of Claim 60, wherein the modulus C is w-little and w-light.

68.(New) A method of encrypting data, comprising:

receiving data; and

using a modulus C to encrypt the data, wherein C is a w-bit number, wherein the modulus C is of the form $2^w - x$, wherein $x = \pm L$, wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$, and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

outputting the encrypted data;

wherein the modulus C is calculated by a process including

(a) providing a number $P < 2^{2w}$;

(b) splitting P into 2 w-bit words H_1 and L_1;

(c) calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$, wherein $(w-3)/2 > x_1 > x_2 > \ldots > x_k > 0$ and $k << w$;

(d) splitting S_1 into two w-bit words H_2 and L_2;

(e) computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

(f) computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$; and

(g) determining the modulus C by comparing S_3 to 2w, wherein the modulus C is a residue, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$.

69.(New) The method of claim 68, wherein the modulus C is w-big.

70.(New) The method of claim 68, wherein the modulus C is w-heavy.

71.(New) The method of claim 68, wherein the modulus C is w-little.

72.(New) The method of claim 68, wherein the modulus C is w-light.

73.(New) The method of claim 68, wherein $x = L$.

74.(New) The method of claim 68, wherein $x = - L$.

75. (New) The method of claim 68, wherein the step of encrypting the data includes the step of performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) converting to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

76. (New) The method of claim 68, wherein the modulus C has a Hamming weight close to 1.

77. (New) The method of Claim 68, wherein the method of encrypting data comprises a method of cryptographic hashing.

78. (New) A method for encrypting data, comprising:

choosing a first basis $(m_1, m_2, \ldots m_t)$ and a second basis $(m_{t+1}, m_{t+2}, \ldots m_{2t})$, wherein $m_1, \ldots, m_{2t}$ are moduli and wherein, for any $m_i \in (m_1, m_2, \ldots m_{2t})$, m_i is a w-bit number selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

encrypting data by performing a ring arithmetic function on numbers by (a) using a residue number multiplication process, (b) converting to the first basis using a mixed radix system, and (c) converting to the second basis using a mixed radix system;

wherein the residue number multiplication process includes

(a) calculating a product $M = m_1 m_2 \ldots m_t$,

(b) calculating a product $W = m_{t+1}m_{t+2} \ldots m_{2t}$, and

(c) calculating a product $ABM^{-1} \bmod p$ for n-bit numbers A and B by

(i) computing Q mod M in the first basis such that $AB + Qp = RM$ for some integral value R and for a number p which is prime relative to M and W;

(ii) converting Q to the second basis, Q mod W, and

(iii) computing R in the second basis, R mod W, wherein $R = (AB + Qp) M^{-1} \bmod W$ and $R \bmod p = ABM^{-1} \bmod p$.

79. (New) The method of claim 78 wherein, for i = 1 to 2t, $2^{k-1} \leq m_i \leq 2^k$, and wherein $m_1, \ldots, m_{2t}$ are pairwise mutually prime.

80. (New) The method of claim 79, wherein $t \geq (n+1)/k$, where n is the bit length of the numbers being multiplied.

81. (New) The method of claim 80, wherein p is an n-bit number, and wherein p is a prime number.

82. (New) The method of claim 78, further comprising converting R to the first basis, R mod M.

83. (New) The method of claim 78, wherein the step of calculating a product $ABM^{-1} \bmod p$ is performed iteratively and includes at least first and second subsequent iterations, and wherein the value of R calculated in the first iteration is utilized as the input value of R in the second iteration.

84. (New) The method of claim 78, wherein the data is encrypted using asymmetric encryption.

85. (New) The method of claim 78, wherein the data is encrypted using symmetric encryption.

86. (New) The method of claim 78, wherein m_i is of the form $2^w + L$, and wherein m_i has a Hamming weight close to 1.

87. (New) The method of Claim 78, wherein m_i is either w-big and w-heavy, or w-little and w-light.